



Don't Touch My Winny

Moti Joseph
moti@gamepe.com

Who Am I?

- Independent Security researcher
- Previously worked at Websense Security Labs, Checkpoint
Hunting for vulnerabilities
Reverse engineering Microsoft patches
Writing plug-in for IDA and OllyDbg
- Mobile developer
- Founder of the XfMobile project www.xf-mobile.com

Agenda

In the next hour, we will cover:

- What is Winny?
- The Story P2P information disclosure in Japan
- Exploiting P2P encrypted traffic

A Day in a life of a Hacker

Reverse engineering , bug hunting, protocol analysis

- Hunting Japanese : Live Demo 0DAY!

NOTE: a talk from a hacker perspective.

Winnie the pooh



Winny

Winny (also known as WinNY) is a Japanese peer-to-peer (P2P) file-sharing program that claims to keep user identities untraceable

The software was developed by Isamu Kaneko

A research in a graduate course of computer engineering at the University of Tokyo in Japan.

He was also once a researcher at the Japan Atomic Energy Research Institute also known as "47-shi" ("Mr. 47").

Winny P2P Software

Winny v2.0b7.1

検索単語: 母乳 ▲検索 ▼検索 Hit: 26 検索トリップ: ▼ BBS ◀ ▶

ノード情報 BBSノード情報 フォルダ情報 **ファイル検索** ダウン条件 無視条件 タスク情報 ログ情報 システム情報

UPフォルダ内 完全キャッシュ 部分キャッシュ **ダウンロード優先度** U: 2 / 0 / 2 10.4K D: 5 / 0 / 2 21.4K 設定

アニメ 母乳 待田来未 上戸彩 Suer

ファイル名	トリップ	サイズ(byte)	ブロック	状態	被参照量(MB)	更新時刻	優先度
【母乳】(姉妹) ホルスタイン県産部 14 ポチャリ可愛い母乳奥さん横水の		697,802,060		仮想ファイル	87	06/07/18 06:56	
(無修正) 巨乳で綺麗なお姉さん(めっちゃめっちゃ美人で母乳出してます)	3VLR44.bTO	510,510,756		仮想ファイル	4,232,118	06/07/18 05:24	
(AV) AROMA (母乳)奥様・母乳搾り008 アンナミラズ制服でコス		508,845,312		仮想ファイル	4,853,125	06/07/18 07:13	
【表】【母乳】Squirting Cow Girl Tits.avi		478,765,080		仮想ファイル	595,557	06/07/18 07:31	
(母乳)【AROMA】奥様母乳搾りJDX02.mpe		407,143,884		完全キャッシュ	1,667,003	06/07/18 05:48	
(母乳)08草アニメ) 乳母 菊池恵.avi		243,916,800		仮想ファイル	802,193	06/07/18 01:50	
(母乳AV)母乳Gカップ 乳搾り 勃起乳首パイプ責めで出るわ出るわ...	ay720GearR	151,487,616		仮想ファイル	943,948	06/07/12 14:54	
【AV】(素人奥様)土下座ナンパ 乳が漏れて母乳が吹きだし止まらなく		101,744,596		仮想ファイル	30,098	06/07/18 06:24	
TV - 母乳 超可愛い素人奥様の出産と授乳シーン (母乳がビューッと		86,175,760		完全キャッシュ	245,771	06/07/16 16:39	
(母乳・姉妹:お宝)TV番組「すくすくネット」もっとおっぱいを知ろう		44,077,056		仮想ファイル	90	06/07/15 02:02	
(母乳・姉妹:お宝)母乳・授乳 若妻おっぱい搾り・乳首ゴコリで恥ずか	NPrWdyxc80	40,658,048		仮想ファイル	116,555	06/07/18 04:28	
(成年コミック)ベガさす百恥辱母乳者.zip	zE79xJ26Ww	19,728,987		仮想ファイル	8,119	06/07/17 11:19	
乳首母乳 NippleMilk(無修正) 姉妹/ハゲ月 姉妹 乳搾り/サーズ/グナ	8V2008.bTO	18,160,426		仮想ファイル	141,717	06/07/18 05:39	
(成人OG集)errors315(母乳・中出し).zip	skpwNM97xW	12,152,369		仮想ファイル	50,242	06/04/28 01:12	
(成年コミック・短編) [山根雄太郎] 愛の醜態 (小学生姉妹、母乳).zip		6,575,877		仮想ファイル	4,305	06/07/18 02:14	
(成年コミック・短編) [ワグナー] ママがはあとおっぱい!! (母子相		3,910,127		仮想ファイル	8,507	06/07/17 02:55	
0800)不知火舞の母乳をぶたが舐める.EXE		360,402		仮想ファイル	45	06/07/18 03:33	
持帰王国母乳が出る女子高生.pe		69,008		仮想ファイル	0	06/07/18 01:16	
(エロ画像)母乳でてる中学生姉妹.pe		35,413		仮想ファイル	0	06/07/18 01:02	
映画BUMPエクストライバー-SOD上田益えびマヨGAMEマブラブwindow		242		仮想ファイル	32	06/07/18 01:42	

ノード情報 BBSノード情報 フォルダ情報 **ファイル検索** ダウン条件 無視条件 タスク情報 ログ情報 システム情報

ダウンロード リスト削除 リスト編集 リスト再読 未変換チェック U: 2 / 0 / 2 10.4K D: 5 / 0 / 2 21.4K 設定

キーワード(ハッシュ)	トリップ	サイズ制限(MB)	ヒット数	ファイル名	カウント	進行状況	残り時間	転送
[AROMA] 奥様母乳搾りコレ		0 - 0	0	[AROMA] 奥様母乳搾りコレ	589,824 / 702,863,692	キー探索中		
乳首母乳 NippleMilk(無修		0 - 0	0	乳首母乳 NippleMilk(無修	196,608 / 18,160,426	キー探索中		

File Search Up 2 / Down 5 Trans Up 0 / 2 Down 0 / 2 Total Up 10.4 / Down 21.4 Kbyte/s

Winny Developer



So what's the story ?

On November 28, 2003, two Japanese users of Winny :

Yoshihiro Inoue, a 41 year-old self employed businessman from Takasaki , and an unemployed 19-year old from Matsuyama ,

were accused of sharing copyrighted material via Winny and admitted to their crimes.

Shortly following the two users' arrests, Kaneko also had his home searched and had the source code of Winny confiscated by the Kyoto Police



Winny Remote Buffer Overflow Vulnerability

Release Date:

April 21, 2006

Date Reported:

March 22, 2006

Patch Development Time (In Days):**Severity:**

High (Remote Code Execution)

Systems Affected:

Winny version 2.0 b7.1 and before

Systems Affected:

Windows NT 4.0

Windows 98 / ME

Windows 2000

Windows XP

Windows 2003

Overview:

eEye Digital Security has discovered a critical vulnerability in Winny, a very popular Japanese P2P application. This vulnerability may allow a remote attacker to overwrite heap memory with user-controlled data and execute arbitrary code in the context of the user who executed the Winny.

Technical Details:

This vulnerability exists in the handling of specific commands provided by the file transfer port. We chose not to provide detailed information about the location of the vulnerability and how to reproduce it because the author has declined to provide a fix (See "Vulnerability History" below). This vulnerability exists within a strcpy(). We can pass a long string argument with some commands into a heap buffer. There is no checking of the length of this input. Depending on the input, this strcpy() will cause one of the following exploitable conditions:

Chapter 1

August 2003 : Several worms called "Antinny" spread on the winny network.

Some versions of ***Antinny*** work as follows:

Upload files in the computer onto the winny network.

Upload screenshots onto an image board.

Denial-of-service attack to a copyright protecting agency web site.

That information includes governmental documents, information about customers, and people's private files.

Chapter 2

Arguably the biggest winny-related leak however, is that of the ***Okayama Police Force***, whose computer leaked data on around 1,500 investigations.

This information included sensitive data , such as the names of sex crime victims, and is the largest amount of information held by Japanese police to have ever leaked online.

December 13, 2006

Winny Developer gets fined \$12,500

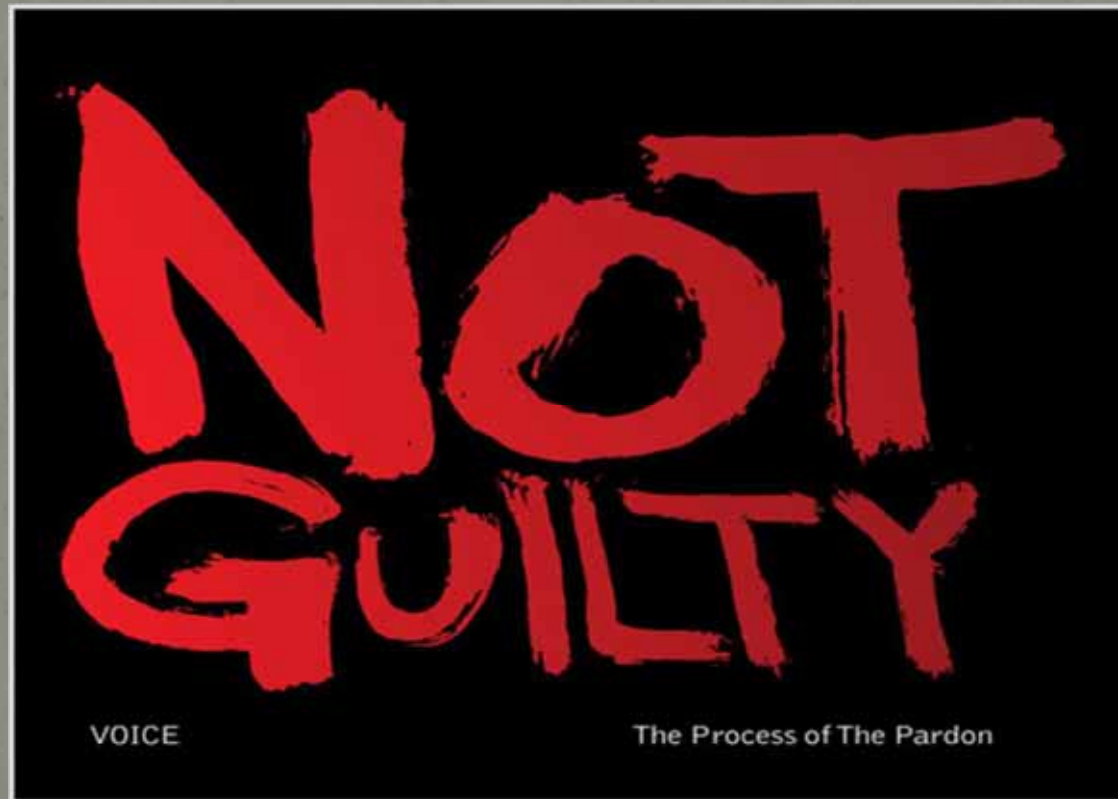
The creator of WinNY, the Japanese [P2P file-sharing program](#), has been convicted in Kyoto District Court of assisting in copyright infringement.



October 8, 2009

Winny Developer found not guilty

Judge Ogura at Osaka High Court found Isamu Kaneko, a developer of Winny, not guilty today, reversing the guilty ruling of 1.5 million yen fine made by the lower court.



April 2010 Winny Trojan

APRIL 23, 2010

JAPANESE RANSOM TROJAN HORSE

This [BBC blog](#) mentioned recently a new threat attacking Japanese users aka "Kenzero" trojan and we would like to clarify some information about it.

AVG detects all known variants as **Trojan horse Generic17.ATLK** and **Trojan horse PSW.Generic7.AUUX**.

This malware belongs to locker or ransom trojan family. Its purpose is to compromise and take ransom from users of infected computer.

It spreads among users of P2P software WinNy. This software is popular amongst the Japanese Hentai collector community. There are more language versions of WinNy. It's popular for illegal content sharing, mostly because WinNy provides partial anonymity for its users. This depends on WinNy version. WinNy has totally 200M users around the world.

Trojan looks like an installation of new Hentai game.



The Story that never been told !!!

0day for the WinNY !

Today i will disclose my private 0day

Universal exploit : stack based buffer overflow

remote code execution

Day in Reverse World

The challenge :

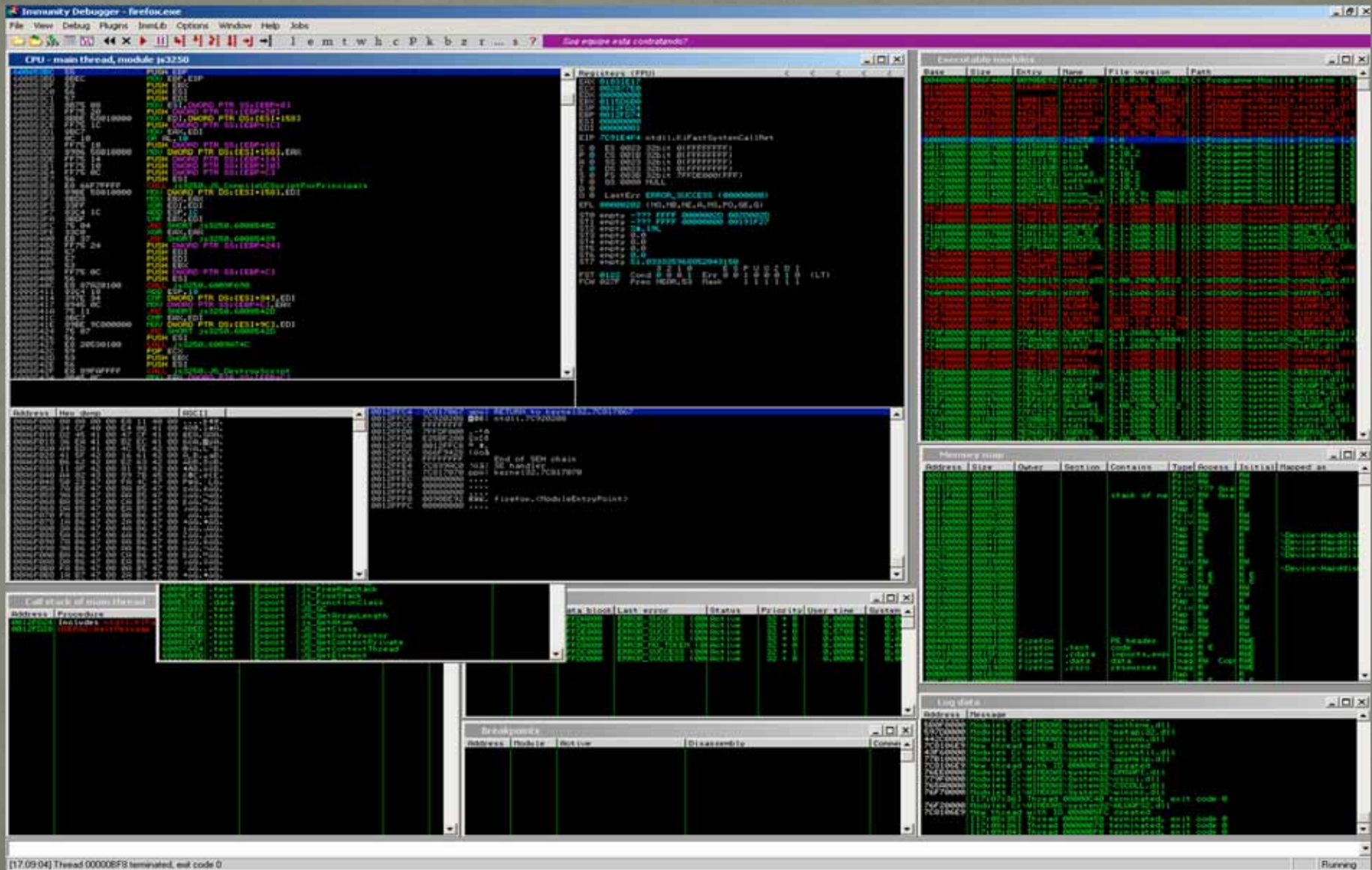
- Reverse engineering
- bug hunting
- protocol analysis
- writing the exploit

Tools we are going to use ...

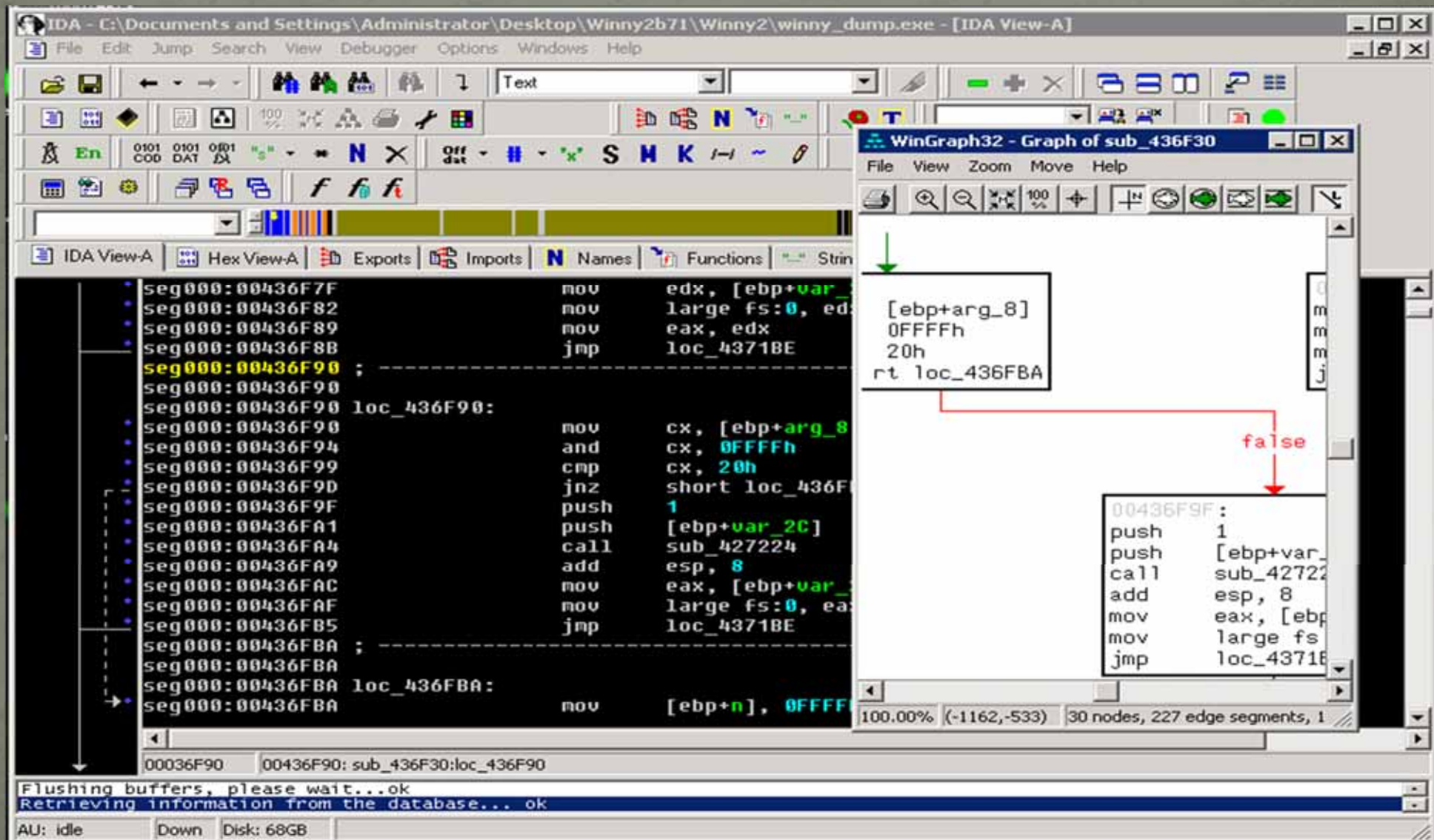


A zero-day (or zero-hour) attack or threat is a computer threat that tries to exploit computer software vulnerabilities which are unknown to others, undisclosed to the software vendor, or without an available security fix

Immunity debugger



IDA PRO 5 DISASSEMBLER



Active Ports

Active Ports								
File Options ?								
Process	P...	Local IP	Local Port	Remote IP	Remote Port	State	Protocol	Path
UDP System	4	192.168.9.99	138			LISTEN	UDP	
UDP System	4	192.168.9.99	137			LISTEN	UDP	
UDP System	4	0.0.0.0	445			LISTEN	UDP	
TCP System	4	192.168.9.99	139			LISTEN	TCP	
TCP System	4	0.0.0.0	445			LISTEN	TCP	
TCP alg.exe	280	127.0.0.1	1026			LISTEN	TCP	C:\WINDC
UDP lsass.exe	652	0.0.0.0	4500			LISTEN	UDP	C:\WINDC
UDP lsass.exe	652	0.0.0.0	500			LISTEN	UDP	C:\WINDC
TCP svchost.exe	804	192.168.9.99	3389	194.29.44.60	2192	ESTABLISHED	TCP	C:\WINDC
TCP svchost.exe	848	192.168.9.99	135	192.168.7.234	1238	ESTABLISHED	TCP	C:\WINDC
UDP svchost.exe	928	192.168.9.99	123			LISTEN	UDP	C:\WINDC
UDP svchost.exe	928	127.0.0.1	1025			LISTEN	UDP	C:\WINDC
UDP svchost.exe	1028	192.168.9.99	1900			LISTEN	UDP	C:\WINDC
TCP WinVNC4.exe	1648	0.0.0.0	5900			LISTEN	TCP	C:\Progran
TCP WinVNC4.exe	1648	0.0.0.0	5800			LISTEN	TCP	C:\Progran
UDP rdpclip.exe	1980	0.0.0.0	1037			LISTEN	UDP	C:\WINDC
UDP idag.exe	2128	0.0.0.0	23945			LISTEN	UDP	C:\Progran
TCP Winny.exe	2700	0.0.0.0	21020			LISTEN	TCP	C:\Docum
TCP Winny.exe	2700	0.0.0.0	17858			LISTEN	TCP	C:\Docum
UDP msnmsgr.exe	3032	127.0.0.1	3322			LISTEN	UDP	C:\Progran
TCP msnmsgr.exe	3032	192.168.9.99	4536	194.29.36.107	8080	ESTABLISHED	TCP	C:\Progran
UDP iexplore.exe	3384	127.0.0.1	3501			LISTEN	UDP	C:\Progran
UDP IEXPLORE.E...	3608	127.0.0.1	3737			LISTEN	UDP	C:\Progran

Terminate Process Query Names

X Exit

Ethereal Network Sniffer

(Untitled) - Ethereal

File Edit View Go Capture Analyze Statistics Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.9.1	224.0.0.10	EIGRP	Hello
2	0.387028	Cisco_54:e9:0d	Spanning-tree-(for	STP	Conf. Root = 8192/00:04:28:b7:88:06 Cost
3	1.167941	Vmware_9a:b4:e6	Broadcast	ARP	who has 192.168.9.1? Tell 192.168.9.249
4	1.168108	Cisco_f6:21:42	Vmware_9a:b4:e6	ARP	192.168.9.1 is at 00:04:27:f6:21:42

Frame 1 (74 bytes on wire, 74 bytes captured)

Ethernet II, Src: Cisco_f6:21:42 (00:04:27:f6:21:42), Dst: 01:00:5e:00:00:0a (01:00:5e:00:00:0a)

Internet Protocol, Src: 192.168.9.1 (192.168.9.1), Dst: 224.0.0.10 (224.0.0.10)

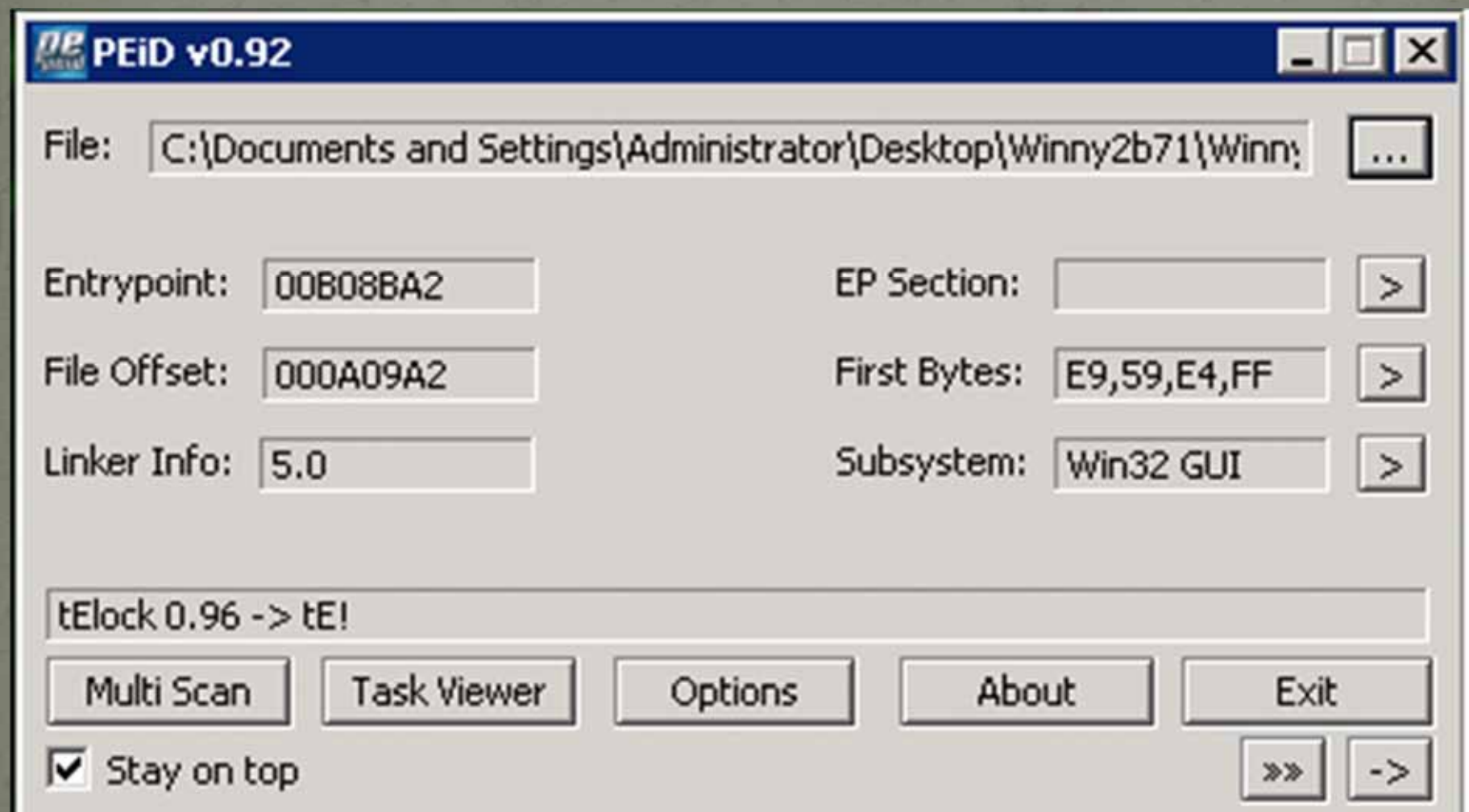
Cisco EIGRP

```

0000  01 00 5e 00 00 0a 00 04 27 f6 21 42 08 00 45 c0  ..A.....!.B..E.
0010  00 3c 00 00 00 00 02 58 0d f7 c0 a8 09 01 e0 00  .<.....X.....
0020  00 0a 02 05 ee ce 00 00 00 00 00 00 00 00 00 00  .....
0030  00 00 00 00 00 01 00 01 00 0c 01 00 01 00 00 00  .....
0040  00 0f 00 04 00 08 0c 01 01 02                    .....
  
```

File: "C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\etherXXXB0LJCT" 342 Bytes 00:00 | P: 4 D: 4 M: 0 Drops: 0

PEiD Packer Detector



Let's go hunting

Binary Audit



LET THE GAME BEGIN

Hunting for 0day Winny Vulnerability

The Plan:

Find out which kind of encryption was used .

Find out where is the vulnerability.

Remotely execute code by exploiting the vulnerability

LET THE GAME BEGIN

Hunting for 0day Vulnerability

The Plan:

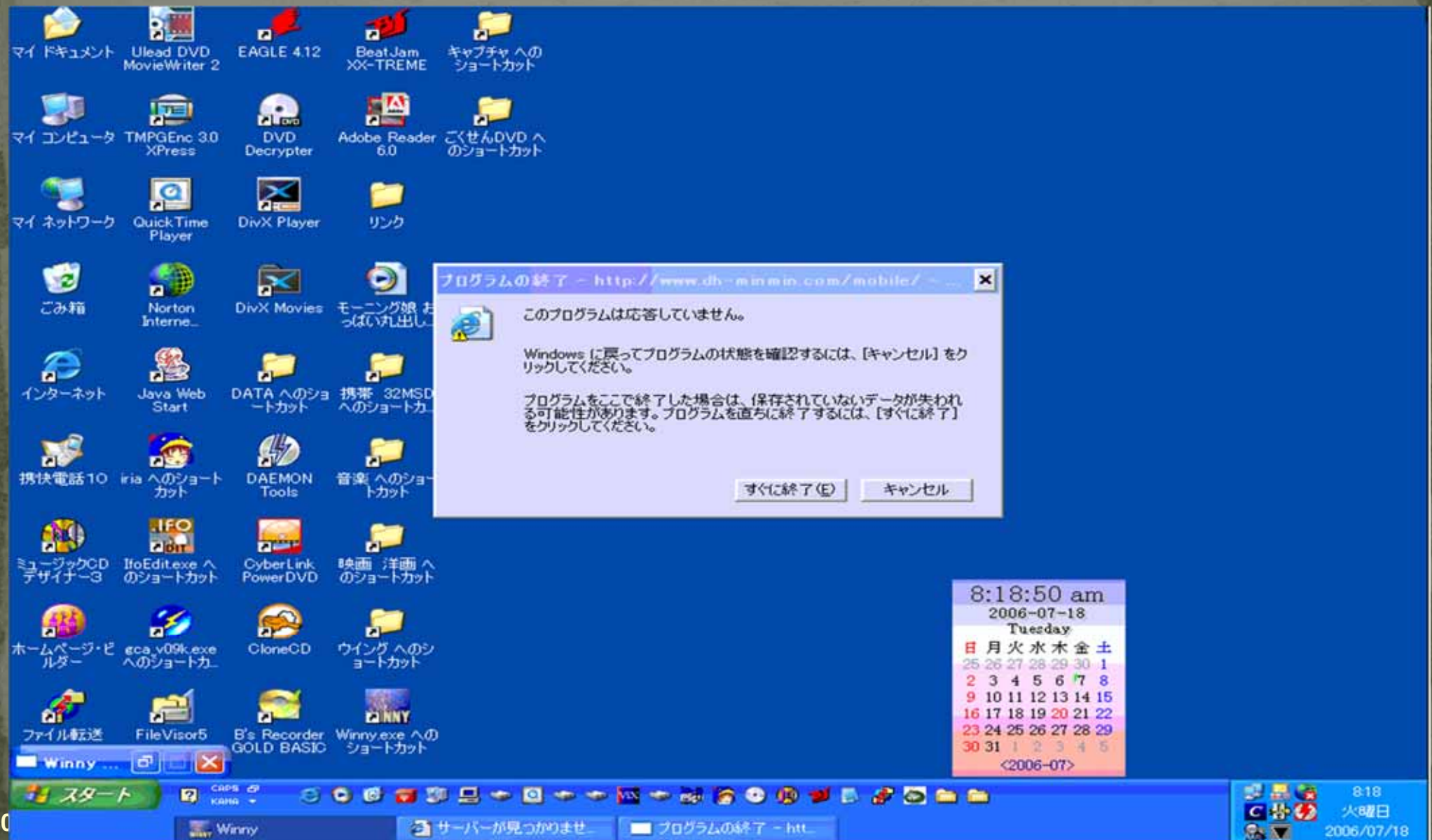
Find out which kind of encryption was used .

Find out where is the vulnerability.

Remotely execute code by exploiting the vulnerability

Live Session/Demo ■

Game Over ! ;)



Credit

Kobi Pariente

Dror Shalev

eEye Digital Security

Check Point

Rivka

Questions?